New Impossible Differential and Known-Key Distinguishers for the 3D Cipher

Jorge Nakahara Jr*

jorge_nakahara@yahoo.com.br

Abstract. The contributions of this paper are new 6-round impossible-differential (ID) and 9.75-round known-key distinguishers for the 3D block cipher. The former was constructed using the miss-in-the-middle technique, while the latter with an inside-out technique. These are the largest ID and known-key distinguishers obtained for the 3D cipher so far, based on the fact that complete diffusion is achieved after three full rounds. Thus, we exploited the slow diffusion in 3D to attack the largest possible number of rounds. The ID distinguishers lead to improved attacks on 10-round variants of the 3D cipher, in the single-key (non related-key) model. These results represent the currently best attacks reported on reduced-round 3D cipher.

Keywords: impossible-differential cryptanalysis, known-key and impossible-differential distinguishers, block ciphers.

1 Introduction

This paper presents new known-key and impossible-differential distinguishers, as well as key-recovery attacks on reduced-round versions of the 3D block cipher [17]. The impossible-differential technique was originally described in [13] and applied to the DEAL block cipher. In [17], an ID attack was presented against 5.75 rounds of 3D (see Table 1), based on a 4.75-round distinguisher.

We describe new 6-round ID distinguishers for 3D, using the miss-in-the-middle technique [4]. We further perform key-recovery attacks on up to 10 rounds. Table 1 summarizes the previous results and the attacks in this paper.

Known-key distinguishers were first presented by Knudsen and Rijmen in [14]. We present new 7.75- and 9.75-round distinguishers for the 3D cipher, which compares favorably when compared with the 7-round distinguisher found for the AES.

This paper is organized as follows: Sect. 2 briefly describes the target cipher; Sect. 3 describes new 6-round ID distinguishers for reduced-round 3D; Sect. 4 describes key-recovery attacks on reduced-round 3D; Sect. 5 describes known-key distinguishers; Sect. 6 concludes this paper.

* This research was conducted while the author was affiliated to École Polytechnique Fédérale de Lausanne, EPFL, Lausanne, Switzerland.

F. Bao and J. Weng (Eds.): ISPEC 2011, LNCS 6672, pp. 208–221, 2011.

2 Brief Description of the 3D Cipher

The 3D block cipher operates on 512-bit blocks under a 512-bit user key, both of which are represented as a $4 \times 4 \times 4$ state of bytes [17]. The three-dimensional cipher state, for a 64-byte data block $A = (a_0, a_1, \ldots, a_{63})$, is denoted

$$\text{State} = \left(\begin{array}{cccc|cccc|cccc|cccc} a_0 & a_4 & a_8 & a_{12} & a_{16} & a_{20} & a_{24} & a_{28} & a_{32} & a_{36} & a_{40} & a_{44} & a_{48} & a_{52} & a_{56} & a_{60} \\ a_1 & a_5 & a_9 & a_{13} & a_{17} & a_{21} & a_{25} & a_{29} & a_{33} & a_{37} & a_{41} & a_{45} & a_{49} & a_{53} & a_{57} & a_{61} \\ a_2 & a_6 & a_{10} & a_{14} & a_{18} & a_{22} & a_{26} & a_{30} & a_{34} & a_{38} & a_{42} & a_{46} & a_{50} & a_{54} & a_{58} & a_{62} \\ a_3 & a_7 & a_{11} & a_{15} & a_{19} & a_{23} & a_{27} & a_{31} & a_{35} & a_{39} & a_{43} & a_{47} & a_{51} & a_{55} & a_{59} & a_{63} \end{array}\right) \quad (1)$$

Bytes are ordered columnwise. The round subkeys follow this same ordering and structure. We denote the first byte of subkey k_i as $k_{i,0}$, the second byte as $k_{i,1}$, and so on. Each set of 16 bytes in a square is called a slice of the state. In total, 3D iterates 22 rounds. The round transformations in 3D have a clear correspondence with those of the AES [9]. Using the terminology of [17]:

- κ_i: bitwise xor with round subkey, equivalent to AddRoundKey in AES;
- γ: a bytewise S-box application, equivalent to SubBytes in AES;
- θ_1, θ_2: equivalent to ShiftRows in AES but applied to each slice of the state alternately; θ_1 in the odd-numbered rounds, θ_2 in the even-numbered rounds;
- π: matrix multiplication with columns of the state, equivalent to MixColumns in AES.

Each round transformation stands for a fraction of 0.25 (a quarter) of a round. Thus, distinguishers may sometimes cover fractions of a round, such as 5.25 rounds, for instance. The key schedule of 3D follows a similar framework as encryption. We refer to [17] for further details.

3 ID Distinguishers

The impossible differential (ID) technique was formerly described in [13]. To construct the new ID distinguishers, truncated differentials and the miss-in-the-middle technique (MITM) [4] were used. The idea of the MITM approach is to concatenate two truncated differentials, say[1], $\alpha \xrightarrow{f} \beta$ and $\epsilon \xleftarrow{g} \eta$, both of which hold with certainty, into a single differential $\alpha \overset{g^{-1} \circ f}{\rightarrow} \eta$, where $g^{-1} \circ f$ stands for the functional composition of f and g^{-1} in this order. Nonetheless, $\beta \neq \epsilon$, that is, the differences do not match in the middle of the distinguisher, which means a contradiction[2]. Consequently, $\alpha \overset{g^{-1} \circ f}{\rightarrow} \eta$ holds with probability zero, or analogously, $\alpha \overset{g^{-1} \circ f}{\not\rightarrow} \eta$ holds

[1] $\alpha \xrightarrow{f} \beta$ means that the difference α causes difference β after the transformation f in the encryption (or forward) direction; $\epsilon \xleftarrow{g} \eta$ means that the difference η causes difference ϵ after the transformation g in the decryption (or backwards) direction. Note the direction of the arrows.

[2] For instance, a zero (byte) difference causes a nonzero (byte) difference (or vice-versa) across a bijective S-box.

with certainty. The terminology $\alpha \overset{g^{-1}\circ f}{\not\rightarrow} \eta$ means that α can never cause the difference η across the transformations $g^{-1} \circ f$ in the encryption direction. Analogously, for the decryption direction. This set of differences α, β, ϵ, η characterize an ID distinguisher constructed with the MITM technique. Once such distinguishers are found, a key-recovery attack can be applied on a few additional rounds before or after the distinguisher. Subkeys are guessed in the rounds before or after the distinguisher, and if they lead to differences α and η then they are wrong keys, because they lead to a contradiction, the impossible differential. The ID attack is a sieving technique: the correct key is recovered indirectly, by eliminating all the wrong keys (the false alarms).

The ID technique has already been applied to many ciphers, including IDEA and Khufu [4], Twofish [5], Rijndael [1,8], CRYPTON [8], Zodiac [12], Hierocrypt-3 [7], TEA and XTEA [16], among others.

Unlike differential cryptanalysis (DC), where we only look for upperbounds on the probability of characteristics or differentials, ID cryptanalysis rather finds lowerbounds (with probability zero). Recall that ID also uses differentials, so it is a kind of DC, as its name indicates. So, as Shamir mentioned[3], it is not enough anymore just to find the highest probability differential to claim that a cipher resists all kinds of DC attacks. Finding lowerbounds on the probability of distinguishers is also very relevant, and this is aim of ID cryptanalysis.

In the distinguishers, the symbol 'Δ' stands for a nonzero byte (xor) difference, also called an active byte; the symbol '0' will stand for the zero byte (xor) difference, also called a passive byte. The symbol '?' denotes either a zero or a nonzero byte difference. Right/left arrows indicate difference propagation (with certainty) in the encryption/decryption directions, respectively. Broken arrows indicate impossible difference propagation. Labels on top of arrows indicate the number of rounds or the round transformations between difference patterns. Sometimes, π and κ_i layers will be swapped, leading to an equivalent subkey, $\kappa_i' = \pi^{-1}(\kappa_i)$, since these transformations are linear. Composition of round transformations is evaluated in right-to-left order both for encryption and decryption operations. For example, for a given state x, $\pi \circ \theta_1 \circ \gamma \circ \kappa_i(x) = \pi(\theta_1(\gamma(\kappa_i(x))))$.

To simplify notation, instead of specifying every round transformation covered by a distinguisher, like $\alpha \overset{g^{-1}\circ f}{\rightarrow} \eta$, we just mention the number of rounds covered, such as $\alpha \overset{3r}{\rightarrow} \eta$, meaning α causes η after three (full) rounds. The distinguisher (2) combines two 3-round truncated differentials: $\alpha \overset{3r}{\rightarrow} \beta$ in the encryption direction and $\epsilon \overset{3r}{\leftarrow} \eta$ in the decryption direction, both holding with certainty. Any placement of the single byte difference in α among the 64 byte positions in the state leads to an equivalent distinguisher. Analogously, there are 64 alternative difference patterns for η, leading to 64 other 6-round ID distinguishers. Thus, in total, we have $64^2 = 2^{12}$ 6-round ID distinguishers following the framework of (2). In summary, a single-byte difference (in any position) in the state cannot cause a single-byte difference after 6-round 3D.

[3] See Adi Shamir's talk at the Rump Session of Crypto'98:
http://en.wikipedia.org/wiki/Impossible_differential_cryptanalysis

The concatenation of $\alpha \xrightarrow{3r} \beta$ and $\epsilon \xleftarrow{3r} \eta$ results in $\alpha \overset{6r}{\not\rightarrow} \eta$ because of a contradiction between the difference patterns in β and ϵ after the third π layer. Before and after this π layer there is a single Δ byte difference in every column. This pattern contradicts the branch number of π which is 5. Contradictions can also be identified in other places along the 6-round distinguisher by extending the two truncated differentials. The same holds in the opposite direction: $\alpha \overset{6r}{\not\leftarrow} \eta$, which might be relevant for attacks in a chosen-ciphertext (CC) setting (see Appendix A).

The rationale for the construction of (2) is the fact that complete diffusion in the 3D cipher requires three full rounds. Note that (2) consists of two truncated differentials, both starting with a single Δ byte and propagating undisturbed until complete diffusion is (almost) achieved.

Unlike conventional ID distinguishers, (2) and (3) have low Hamming weight both for α and for η, concerning byte differences, that is, there are too many zero byte differences in α and η. This fact makes the new distinguishers ineffective in attacks like [4,6]. Rather, we use the technique in [1] to accomplish key-recovery attacks. These new constructions compare favorably with the ID distinguisher described in [17], in which the Hamming weight of the input and output differences was significantly higher.

$$
\alpha = \left(\begin{array}{c|c|c|c} \Delta\,0\,0\,0 & 0\,0\,0\,0 & 0\,0\,0\,0 & 0\,0\,0\,0 \\ 0\,0\,0\,0 & 0\,0\,0\,0 & 0\,0\,0\,0 & 0\,0\,0\,0 \\ 0\,0\,0\,0 & 0\,0\,0\,0 & 0\,0\,0\,0 & 0\,0\,0\,0 \\ 0\,0\,0\,0 & 0\,0\,0\,0 & 0\,0\,0\,0 & 0\,0\,0\,0 \end{array}\right)
\xrightarrow{\pi\circ\theta_1\circ\gamma\circ\kappa_i}
\left(\begin{array}{c|c|c|c} \Delta\,0\,0\,0 & 0\,0\,0\,0 & 0\,0\,0\,0 & 0\,0\,0\,0 \\ \Delta\,0\,0\,0 & 0\,0\,0\,0 & 0\,0\,0\,0 & 0\,0\,0\,0 \\ \Delta\,0\,0\,0 & 0\,0\,0\,0 & 0\,0\,0\,0 & 0\,0\,0\,0 \\ \Delta\,0\,0\,0 & 0\,0\,0\,0 & 0\,0\,0\,0 & 0\,0\,0\,0 \end{array}\right)
$$

$$
\xrightarrow{\theta_2\circ\gamma\circ\kappa_{i+1}}
\left(\begin{array}{c|c|c|c} \Delta\,0\,0\,0 & 0\,0\,0\,0 & 0\,0\,0\,0 & 0\,0\,0\,0 \\ 0\,0\,0\,0 & 0\,0\,0\,0 & 0\,0\,0\,0 & \Delta\,0\,0\,0 \\ 0\,0\,0\,0 & 0\,0\,0\,0 & \Delta\,0\,0\,0 & 0\,0\,0\,0 \\ 0\,0\,0\,0 & \Delta\,0\,0\,0 & 0\,0\,0\,0 & 0\,0\,0\,0 \end{array}\right)
\xrightarrow{\pi}
\left(\begin{array}{c|c|c|c} \Delta\,0\,0\,0 & \Delta\,0\,0\,0 & \Delta\,0\,0\,0 & \Delta\,0\,0\,0 \\ \Delta\,0\,0\,0 & \Delta\,0\,0\,0 & \Delta\,0\,0\,0 & \Delta\,0\,0\,0 \\ \Delta\,0\,0\,0 & \Delta\,0\,0\,0 & \Delta\,0\,0\,0 & \Delta\,0\,0\,0 \\ \Delta\,0\,0\,0 & \Delta\,0\,0\,0 & \Delta\,0\,0\,0 & \Delta\,0\,0\,0 \end{array}\right)
$$

$$
\xrightarrow{\theta_1\circ\gamma\circ\kappa_{i+2}}
\left(\begin{array}{c|c|c|c} \Delta\,0\,0\,0 & \Delta\,0\,0\,0 & \Delta\,0\,0\,0 & \Delta\,0\,0\,0 \\ 0\,0\,0\,\Delta & 0\,0\,0\,\Delta & 0\,0\,0\,\Delta & 0\,0\,0\,\Delta \\ 0\,0\,\Delta\,0 & 0\,0\,\Delta\,0 & 0\,0\,\Delta\,0 & 0\,0\,\Delta\,0 \\ 0\,\Delta\,0\,0 & 0\,\Delta\,0\,0 & 0\,\Delta\,0\,0 & 0\,\Delta\,0\,0 \end{array}\right)
\overset{\pi}{\not\rightarrow}
$$

$$
\left(\begin{array}{c|c|c|c} \Delta\,\Delta\,\Delta\,\Delta & 0\,0\,0\,0 & 0\,0\,0\,0 & 0\,0\,0\,0 \\ 0\,0\,0\,0 & \Delta\,\Delta\,\Delta\,\Delta & 0\,0\,0\,0 & 0\,0\,0\,0 \\ 0\,0\,0\,0 & 0\,0\,0\,0 & \Delta\,\Delta\,\Delta\,\Delta & 0\,0\,0\,0 \\ 0\,0\,0\,0 & 0\,0\,0\,0 & 0\,0\,0\,0 & \Delta\,\Delta\,\Delta\,\Delta \end{array}\right)
\xleftarrow{\kappa_{i+3}\circ\gamma^{-1}\circ\theta_2^{-1}}
$$

$$
\left(\begin{array}{c|c|c|c} \Delta\,\Delta\,\Delta\,\Delta & 0\,0\,0\,0 & 0\,0\,0\,0 & 0\,0\,0\,0 \\ \Delta\,\Delta\,\Delta\,\Delta & 0\,0\,0\,0 & 0\,0\,0\,0 & 0\,0\,0\,0 \\ \Delta\,\Delta\,\Delta\,\Delta & 0\,0\,0\,0 & 0\,0\,0\,0 & 0\,0\,0\,0 \\ \Delta\,\Delta\,\Delta\,\Delta & 0\,0\,0\,0 & 0\,0\,0\,0 & 0\,0\,0\,0 \end{array}\right)
\xleftarrow{\pi^{-1}}
$$

$$
\left(\begin{array}{c|c|c|c} \Delta\,0\,0\,0 & 0\,0\,0\,0 & 0\,0\,0\,0 & 0\,0\,0\,0 \\ 0\,\Delta\,0\,0 & 0\,0\,0\,0 & 0\,0\,0\,0 & 0\,0\,0\,0 \\ 0\,0\,\Delta\,0 & 0\,0\,0\,0 & 0\,0\,0\,0 & 0\,0\,0\,0 \\ 0\,0\,0\,\Delta & 0\,0\,0\,0 & 0\,0\,0\,0 & 0\,0\,0\,0 \end{array}\right)
\xleftarrow{\kappa_{i+4}\circ\gamma^{-1}\circ\theta_1^{-1}}
\left(\begin{array}{c|c|c|c} \Delta\,0\,0\,0 & 0\,0\,0\,0 & 0\,0\,0\,0 & 0\,0\,0\,0 \\ \Delta\,0\,0\,0 & 0\,0\,0\,0 & 0\,0\,0\,0 & 0\,0\,0\,0 \\ \Delta\,0\,0\,0 & 0\,0\,0\,0 & 0\,0\,0\,0 & 0\,0\,0\,0 \\ \Delta\,0\,0\,0 & 0\,0\,0\,0 & 0\,0\,0\,0 & 0\,0\,0\,0 \end{array}\right)
$$

$$
\xleftarrow{\pi^{-1}\circ\kappa_{i+5}\circ\gamma^{-1}\circ\theta_2^{-1}\circ\kappa_{i+6}}
\left(\begin{array}{c|c|c|c} \Delta\,0\,0\,0 & 0\,0\,0\,0 & 0\,0\,0\,0 & 0\,0\,0\,0 \\ 0\,0\,0\,0 & 0\,0\,0\,0 & 0\,0\,0\,0 & 0\,0\,0\,0 \\ 0\,0\,0\,0 & 0\,0\,0\,0 & 0\,0\,0\,0 & 0\,0\,0\,0 \\ 0\,0\,0\,0 & 0\,0\,0\,0 & 0\,0\,0\,0 & 0\,0\,0\,0 \end{array}\right) = \eta
\tag{2}
$$

Note that (2) starts from a round using θ_1. Since 3D contains two kinds of byte permutation, θ_1 and θ_2, an equivalent 6-round ID distinguisher is presented in (3), for attacks starting with θ_2.

$$\alpha' = \left(\begin{array}{cccc|cccc|cccc|cccc} \Delta&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0 \end{array}\right) \overset{\pi\circ\theta_2\circ\gamma\circ\kappa_i}{\rightarrow} \left(\begin{array}{cccc|cccc|cccc|cccc} \Delta&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\ \Delta&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\ \Delta&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\ \Delta&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0 \end{array}\right)$$

$$\overset{\theta_1\circ\gamma\circ\kappa_{i+1}}{\rightarrow} \left(\begin{array}{cccc|cccc|cccc|cccc} \Delta&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\ 0&0&0&\Delta&0&0&0&0&0&0&0&0&0&0&0&0\\ 0&0&\Delta&0&0&0&0&0&0&0&0&0&0&0&0&0\\ 0&\Delta&0&0&0&0&0&0&0&0&0&0&0&0&0&0 \end{array}\right) \overset{\pi}{\rightarrow} \left(\begin{array}{cccc|cccc|cccc|cccc} \Delta&\Delta&\Delta&\Delta&0&0&0&0&0&0&0&0&0&0&0&0\\ \Delta&\Delta&\Delta&\Delta&0&0&0&0&0&0&0&0&0&0&0&0\\ \Delta&\Delta&\Delta&\Delta&0&0&0&0&0&0&0&0&0&0&0&0\\ \Delta&\Delta&\Delta&\Delta&0&0&0&0&0&0&0&0&0&0&0&0 \end{array}\right)$$

$$\overset{\theta_2\circ\gamma\circ\kappa_{i+2}}{\rightarrow} \left(\begin{array}{cccc|cccc|cccc|cccc} \Delta&\Delta&\Delta&\Delta&0&0&0&0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0&0&0&0&\Delta&\Delta&\Delta&\Delta\\ 0&0&0&0&0&0&0&0&\Delta&\Delta&\Delta&\Delta&0&0&0&0\\ 0&0&0&0&\Delta&\Delta&\Delta&\Delta&0&0&0&0&0&0&0&0 \end{array}\right) \overset{\theta_1\circ\gamma\circ\kappa_{i+3}\circ\pi}{\rightarrow}$$

$$\left(\begin{array}{cccc|cccc|cccc|cccc} \Delta&\Delta&\Delta&\Delta&\Delta&\Delta&\Delta&\Delta&\Delta&\Delta&\Delta&\Delta&\Delta&\Delta&\Delta&\Delta\\ \Delta&\Delta&\Delta&\Delta&\Delta&\Delta&\Delta&\Delta&\Delta&\Delta&\Delta&\Delta&\Delta&\Delta&\Delta&\Delta\\ \Delta&\Delta&\Delta&\Delta&\Delta&\Delta&\Delta&\Delta&\Delta&\Delta&\Delta&\Delta&\Delta&\Delta&\Delta&\Delta\\ \Delta&\Delta&\Delta&\Delta&\Delta&\Delta&\Delta&\Delta&\Delta&\Delta&\Delta&\Delta&\Delta&\Delta&\Delta&\Delta \end{array}\right) \overset{\pi^{-1}}{\not\leftarrow}$$

$$\left(\begin{array}{cccc|cccc|cccc|cccc} 0&0&0&0&0&0&0&0&0&0&0&0&\Delta&0&0&0\\ \Delta&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\ 0&0&0&0&\Delta&0&0&0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&\Delta&0&0&0&0&0&0&0 \end{array}\right) \overset{\kappa_{i+4}\circ\gamma^{-1}\circ\theta_2^{-1}}{\leftarrow} \left(\begin{array}{cccc|cccc|cccc|cccc} 0&0&0&0&0&0&0&0&0&0&0&0&\Delta&0&0&0\\ 0&0&0&0&0&0&0&0&0&0&0&0&\Delta&0&0&0\\ 0&0&0&0&0&0&0&0&0&0&0&0&\Delta&0&0&0\\ 0&0&0&0&0&0&0&0&0&0&0&0&\Delta&0&0&0 \end{array}\right)$$

$$\overset{\pi^{-1}\circ\kappa_{i+5}\circ\gamma^{-1}\circ\theta_1^{-1}\circ\kappa_{i+6}}{\leftarrow} \left(\begin{array}{cccc|cccc|cccc|cccc} 0&0&0&0&0&0&0&0&0&0&0&0&\Delta&0&0&0\\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0 \end{array}\right) = \eta'$$

(3)

4 ID Attack on 10-Round 3D

We describe a key-recovery attack on 10-round 3D by placing (2) in the third round (or any other round farther as long as it uses θ_1) and recovering subkey bits from k_0, k_1, k_9 and k_{10}. The attack framework is depicted in (4), where '*' means byte positions that have to be known to allow partial encryption/decryption, such as text and subkey bytes.

$$\left(\begin{array}{cccc|cccc|cccc|cccc} *&0&0&0&*&0&0&0&*&0&0&0&*&0&0&0\\ 0&*&0&0&0&*&0&0&0&*&0&0&0&*&0&0\\ 0&0&*&0&0&0&*&0&0&0&*&0&0&0&*&0\\ 0&0&0&*&0&0&0&*&0&0&0&*&0&0&0&* \end{array}\right) \overset{\theta_1\circ\gamma\circ\kappa_0}{\rightarrow} \left(\begin{array}{cccc|cccc|cccc|cccc} *&0&0&0&*&0&0&0&*&0&0&0&*&0&0&0\\ *&0&0&0&*&0&0&0&*&0&0&0&*&0&0&0\\ *&0&0&0&*&0&0&0&*&0&0&0&*&0&0&0\\ *&0&0&0&*&0&0&0&*&0&0&0&*&0&0&0 \end{array}\right) \overset{\pi}{\rightarrow}$$

$$\left(\begin{array}{cccc|cccc|cccc|cccc} *&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\ 0&0&0&0&*&0&0&0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&*&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0&0&0&0&*&0&0&0 \end{array}\right) \overset{\theta_2\circ\gamma\circ\kappa_1}{\rightarrow} \left(\begin{array}{cccc|cccc|cccc|cccc} *&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\ *&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\ *&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\ *&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0 \end{array}\right)$$

$$\overset{\pi}{\rightarrow} \text{6-round ID distinguisher} \overset{\pi^{-1}}{\leftarrow} \left(\begin{array}{cccc|cccc|cccc|cccc} *&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\ *&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\ *&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\ *&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0 \end{array}\right)$$

$$\overset{\gamma^{-1}\circ\theta_1^{-1}}{\leftarrow} \left(\begin{array}{cccc|cccc|cccc|cccc} *&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\ 0&0&0&*&0&0&0&0&0&0&0&0&0&0&0&0\\ 0&0&*&0&0&0&0&0&0&0&0&0&0&0&0&0\\ 0&*&0&0&0&0&0&0&0&0&0&0&0&0&0&0 \end{array}\right) \overset{\pi^{-1}\circ\kappa_9}{\leftarrow}$$

$$\left(\begin{array}{cccc|cccc|cccc|cccc} *&*&*&*&0&0&0&0&0&0&0&0&0&0&0&0\\ *&*&*&*&0&0&0&0&0&0&0&0&0&0&0&0\\ *&*&*&*&0&0&0&0&0&0&0&0&0&0&0&0\\ *&*&*&*&0&0&0&0&0&0&0&0&0&0&0&0 \end{array}\right) \overset{\gamma^{-1}\circ\theta_2^{-1}\circ\kappa_{10}}{\leftarrow} \left(\begin{array}{cccc|cccc|cccc|cccc} *&*&*&*&0&0&0&0&0&0&0&0&0&0&0&0\\ 0&0&0&0&*&*&*&*&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&*&*&*&*&0&0&0&0\\ 0&0&0&0&0&0&0&0&0&0&0&0&*&*&*&* \end{array}\right)$$

(4)

The attack steps are the following:

(a) consider 2^n structures, each of which contains 2^{128} plaintexts, with all possible values in diagonal positions of the plaintext state according to (1). That means bytes in positions 0, 5, 10, 15, 16, 21, 26, 31, 32, 37, 42, 47, 48, 53, 58 and 63 of the plaintext state, and fixed values for the remaining bytes. This means about 2^{255} text pairs per structure, and 2^{n+128} plaintexts in total. Request the 10-round encryption of the 2^{n+128} plaintexts (from the 1st round). Filter the ciphertext pairs that have zero byte differences in the 48 ciphertext positions marked with '0' in (4). It is expected that $2^{n+255}(2^{-8})^{48} = 2^{n-129}$ pairs will satisfy this condition.

(b) guess the twenty subkey bytes $k_{10,0}$, $k_{10,4}$, $k_{10,8}$, $k_{10,12}$, $k_{10,17}$, $k_{10,21}$, $k_{10,25}$, $k_{10,29}$, $k_{10,34}$, $k_{10,38}$, $k_{10,42}$, $k_{10,46}$, $k_{10,51}$, $k_{10,55}$, $k_{10,59}$, $k_{10,63}$, $k_{9,0}$, $k_{9,13}$, $k_{9,10}$, $k_{9,7}$, and partially decrypt $\pi^{-1} \circ \gamma^{-1} \circ \theta_1^{-1} \circ \pi^{-1} \circ \kappa_9 \circ \gamma^{-1} \circ \theta_2^{-1} \circ \kappa_{10}$ until one end of the distinguisher. For the transition from the last to the penultimate round, choose text pairs that lead to a single active byte in the leftmost column of each slice, as shown in (4). This is expected to happen with probability $(2^{-24})^4 = 2^{-96}$. Thus, the number of pairs becomes $2^{n-129-96} = 2^{n-225}$. Further, choose among the surviving pairs those whose difference is nonzero in a single byte in the leftmost column of the state, as in the output difference of (2), after the partial 2-round decryption. The probability of such a difference is $(2^{-8})^3 \cdot 4 = 2^{-22}$ since the active byte can be in any position in the column.

(c) guess the twenty subkey bytes $k_{0,0}$, $k_{0,5}$, $k_{0,10}$, $k_{0,15}$, $k_{0,16}$, $k_{0,21}$, $k_{0,26}$, $k_{0,31}$, $k_{0,32}$, $k_{0,37}$, $k_{0,42}$, $k_{0,47}$, $k_{0,48}$, $k_{0,53}$, $k_{0,58}$, $k_{0,63}$, $k_{1,0}$, $k_{1,17}$, $k_{1,34}$, $k_{1,51}$, and partially encrypt $\pi \circ \theta_2 \circ \gamma \circ \kappa_1 \circ \pi \circ \theta_1 \circ \gamma \circ \kappa_0$. In the transition from the 1st to the 2nd round, chose those pairs that lead to the difference pattern with a single active byte in each column of the first slice, as shown in (4). This is expected to happen with probability $(2^{-24})^4 = 2^{-96}$. Thus, the number of pairs becomes $2^{n-225-96} = 2^{n-321}$. Further, with probability $4 \cdot 2^{-24} = 2^{-22}$, we expect to get zero difference in three out of the four byte positions in a column, as in the input difference of (2), after the 2-round partial encryption.

Each text pair defines a set of wrong 40-byte subkeys. The number of surviving wrong subkeys is $2^{40 \cdot 8}(1-2^{-22 \cdot 2})^{2^{n-321}} = 2^{320}(1-2^{-44})^{2^{n-321}}$. Using $n > 372.79$, no wrong subkeys remain. This implies $2^{373+128} = 2^{501}$ chosen plaintexts (CP).

In step (a), the adversary requests the encryption of chosen plaintexts to the legitimate users, since he does not know the key. Thus, there is no computational effort for the adversary in this step. The complexity of step (b) consists of partial 2-round decryption for each subkey guess and valid pair, which means $2^{n-129} \cdot \frac{20}{64} \cdot 2^{160} \cdot 2 = 5 \cdot 2^{n+28}$ 2-round computations, since roughly 20 bytes out of the 64 in a round are computed. For $n = 373$, this corresponds to $5 \cdot 2^{401}/5 = 2^{401}$ 10-round computations. In step (c), 2^{n-225} pairs are analyzed, and for each guess of 20 subkey bytes, two rounds are partially encrypted. This mean

$2^{n-225} \cdot \frac{20}{64} \cdot 2^{160} \cdot 2 = 5 \cdot 2^{n-69}$ 2-round computations. For $n = 373$, the effort is equivalent to $5 \cdot 2^{304}/5 = 2^{304}$ 10-round computations. Overall, the time complexity is 2^{401} 10-round computation.

To keep track of wrong 40-byte subkeys, a storage of $2^{40 \cdot 8}/512 = 2^{311}$ blocks is used. To recover the rest of the key, the same attack can be repeated but only for the remaining bytes of k_9 and k_{10} using the same plaintexts. Thus, no additional chosen plaintexts will be needed. This way, less subkeys are recovered at a time and this residual complexity will not affect the overall time complexity. Once one full 512-bit round subkey is recovered, the original user key can be reconstructed at once, using the key schedule of 3D [17].

5 Known-Key Distinguishers

In this section, we apply the ideas from [14] to reduced-round 3D, due to similarities with the AES. Note that a known-key distinguisher is derived from an inside-out technique, in contrast to an impossible-differential which typically uses the miss-in-the-middle or an outside-in technique. Thus, these distinguishers exploit differentials in opposite directions.

We follow the terminology of multiset or integral attacks, where 'A' stands for an active byte, 'P' stands for a passive byte, 'B' stands for a balanced byte, and '?' stands for a non-balanced byte [10]. The propagation and transformation of different word bytes in a multiset is the same as in SQUARE [10] and AES ciphers, and is a consequence of the fact that wordwise operations in 3D are neatly performed bytewise.

We start with a single 'A' byte in the ith round, in the middle of a state (while the remaining 63 bytes are 'P'). Across 4.25 rounds in the encryption direction, this distinguisher propagates undisturbed (i.e it holds with certainty), ending with 64 'B' bytes (5). After 4.25 rounds, there is a γ layer, and all bytes become '?'. In the decryption direction, again starting from the ith round and propagating freely, we arrive at a state with only 'B' bytes after 3.75 rounds: the upper part of (5). These two pieces form a 7.75-round known-key distinguisher holding with certainty. Similar distinguishers can be obtained if the single 'A' byte was in any of the other 63 position of the ith round in the state. This known-key distinguisher lead to an attack costing 2^8 CP. The time complexity is only 2^8 encryptions and the memory is negligible.

Just like in the ID distinguisher case, we exploited full diffusion of 3D in both the encryption and decryption directions at once in the distinguisher (5). Note the direction of arrows between round transitions. But, unlike the ID case, in the multiset case the 'A' words become 'B' before turning into '?' after about one round, giving almost an additional round at both ends of the distinguisher.

A fundamental assumption for this attack is that the key is known. The attack starts with a single 'A' byte in the middle of 7.75-round 3D cipher. The outcome of the attack is verified by checking if all bytes (at both ends of the

distinguisher) are balanced, which means the xor sum is zero in 512 bits of plaintext and ciphertext's multisets. This assumption may be justified in a hash function setting where the key input is the message input and is under control of an adversary. Nonetheless, the relevance of known-key attacks on r-round 3D is that, for instance, r-round 3D does not behave ideally that is, cannot be modeled as a random permutation. In particular, for (5), the zero xor-sum is expected to happen with probability 2^{-512} for a random permutation, but in 7.75-round 3D cipher, the xor-sum is always zero for any (known) key.

$$
\begin{array}{c}
\left(\begin{array}{cccc|cccc|cccc|cccc}
B&B&B&B&B&B&B&B&B&B&B&B&B&B&B&B\\
B&B&B&B&B&B&B&B&B&B&B&B&B&B&B&B\\
B&B&B&B&B&B&B&B&B&B&B&B&B&B&B&B\\
B&B&B&B&B&B&B&B&B&B&B&B&B&B&B&B
\end{array}\right)\ \theta_1^{-1}\circ\pi^{-1}\circ\kappa_{i-3}\circ\gamma^{-1}\circ\theta_2^{-1}\\
\xleftarrow{}\\
\left(\begin{array}{cccc|cccc|cccc|cccc}
A&A&A&A&A&A&A&A&A&A&A&A&A&A&A&A\\
A&A&A&A&A&A&A&A&A&A&A&A&A&A&A&A\\
A&A&A&A&A&A&A&A&A&A&A&A&A&A&A&A\\
A&A&A&A&A&A&A&A&A&A&A&A&A&A&A&A
\end{array}\right)\ \pi^{-1}\\
\xleftarrow{}\\
\left(\begin{array}{cccc|cccc|cccc|cccc}
A&P&P&P&A&P&P&P&A&P&P&P&A&P&P&P\\
P&A&P&P&P&A&P&P&P&A&P&P&P&A&P&P\\
P&P&A&P&P&P&A&P&P&P&A&P&P&P&A&P\\
P&P&P&A&P&P&P&A&P&P&P&A&P&P&P&A
\end{array}\right)\ \kappa_{i-2}\circ\gamma^{-1}\circ\theta_1^{-1}\\
\xleftarrow{}\\
\left(\begin{array}{cccc|cccc|cccc|cccc}
A&P&P&P&A&P&P&P&A&P&P&P&A&P&P&P\\
A&P&P&P&A&P&P&P&A&P&P&P&A&P&P&P\\
A&P&P&P&A&P&P&P&A&P&P&P&A&P&P&P\\
A&P&P&P&A&P&P&P&A&P&P&P&A&P&P&P
\end{array}\right)\ \pi^{-1}\\
\xleftarrow{}\\
\left(\begin{array}{cccc|cccc|cccc|cccc}
A&P&P&P&P&P&P&P&P&P&P&P&P&P&P&P\\
P&P&P&P&A&P&P&P&P&P&P&P&P&P&P&P\\
P&P&P&P&P&P&P&P&A&P&P&P&P&P&P&P\\
P&P&P&P&P&P&P&P&P&P&P&P&A&P&P&P
\end{array}\right)\ \kappa_{i-1}\circ\gamma^{-1}\circ\theta_2^{-1}\\
\xleftarrow{}\\
\left(\begin{array}{cccc|cccc|cccc|cccc}
A&P&P&P&P&P&P&P&P&P&P&P&P&P&P&P\\
A&P&P&P&P&P&P&P&P&P&P&P&P&P&P&P\\
A&P&P&P&P&P&P&P&P&P&P&P&P&P&P&P\\
A&P&P&P&P&P&P&P&P&P&P&P&P&P&P&P
\end{array}\right)\ \pi^{-1}\\
\xleftarrow{}\\
\left(\begin{array}{cccc|cccc|cccc|cccc}
\mathbf{A}&P&P&P&P&P&P&P&P&P&P&P&P&P&P&P\\
P&P&P&P&P&P&P&P&P&P&P&P&P&P&P&P\\
P&P&P&P&P&P&P&P&P&P&P&P&P&P&P&P\\
P&P&P&P&P&P&P&P&P&P&P&P&P&P&P&P
\end{array}\right)\ \pi\circ\theta_1\circ\gamma\circ\kappa_i\ \longrightarrow\ \left(\begin{array}{cccc|cccc|cccc|cccc}
A&P&P&P&P&P&P&P&P&P&P&P&P&P&P&P\\
A&P&P&P&P&P&P&P&P&P&P&P&P&P&P&P\\
A&P&P&P&P&P&P&P&P&P&P&P&P&P&P&P\\
A&P&P&P&P&P&P&P&P&P&P&P&P&P&P&P
\end{array}\right)\\
\theta_2\circ\gamma\circ\kappa_{i+1}\ \longrightarrow\ \left(\begin{array}{cccc|cccc|cccc|cccc}
A&P&P&P&P&P&P&P&P&P&P&P&P&P&P&P\\
P&P&P&P&P&P&P&P&P&P&P&P&A&P&P&P\\
P&P&P&P&P&P&P&P&A&P&P&P&P&P&P&P\\
P&P&P&P&A&P&P&P&P&P&P&P&P&P&P&P
\end{array}\right)\ \xrightarrow{\pi}\\
\left(\begin{array}{cccc|cccc|cccc|cccc}
A&P&P&P&A&P&P&P&A&P&P&P&A&P&P&P\\
A&P&P&P&A&P&P&P&A&P&P&P&A&P&P&P\\
A&P&P&P&A&P&P&P&A&P&P&P&A&P&P&P\\
A&P&P&P&A&P&P&P&A&P&P&P&A&P&P&P
\end{array}\right)\ \theta_1\circ\gamma\circ\kappa_{i+2}\ \longrightarrow\ \left(\begin{array}{cccc|cccc|cccc|cccc}
A&P&P&P&A&P&P&P&A&P&P&P&A&P&P&P\\
P&P&P&A&P&P&P&A&P&P&P&A&P&P&P&A\\
P&P&A&P&P&P&A&P&P&P&A&P&P&P&A&P\\
P&A&P&P&P&A&P&P&P&A&P&P&P&A&P&P
\end{array}\right)\\
\xrightarrow{\pi}\ \left(\begin{array}{cccc|cccc|cccc|cccc}
A&A&A&A&A&A&A&A&A&A&A&A&A&A&A&A\\
A&A&A&A&A&A&A&A&A&A&A&A&A&A&A&A\\
A&A&A&A&A&A&A&A&A&A&A&A&A&A&A&A\\
A&A&A&A&A&A&A&A&A&A&A&A&A&A&A&A
\end{array}\right)\ \kappa_{i+4}\circ\pi\circ\theta_2\circ\gamma\circ\kappa_{i+3}\ \longrightarrow\\
\left(\begin{array}{cccc|cccc|cccc|cccc}
B&B&B&B&B&B&B&B&B&B&B&B&B&B&B&B\\
B&B&B&B&B&B&B&B&B&B&B&B&B&B&B&B\\
B&B&B&B&B&B&B&B&B&B&B&B&B&B&B&B\\
B&B&B&B&B&B&B&B&B&B&B&B&B&B&B&B
\end{array}\right)
\end{array}
\tag{5}
$$

Analogously, if the forward part (in the encryption direction) started from an odd-numbered round, that is, with θ_2, instead of θ_1, then we would obtain a similar 7.75-round distinguisher, (6).

$$
\begin{array}{c}
\left(\begin{array}{cccc|cccc|cccc|cccc}
B&B&B&B&B&B&B&B&B&B&B&B&B&B&B&B\\
B&B&B&B&B&B&B&B&B&B&B&B&B&B&B&B\\
B&B&B&B&B&B&B&B&B&B&B&B&B&B&B&B\\
B&B&B&B&B&B&B&B&B&B&B&B&B&B&B&B
\end{array}\right) \theta_1^{-1}\circ\pi^{-1}\circ\kappa_{i-3}\circ\gamma^{-1}\circ\theta_1^{-1} \\
\xleftarrow{} \\
\left(\begin{array}{cccc|cccc|cccc|cccc}
A&A&A&A&A&A&A&A&A&A&A&A&A&A&A&A\\
A&A&A&A&A&A&A&A&A&A&A&A&A&A&A&A\\
A&A&A&A&A&A&A&A&A&A&A&A&A&A&A&A\\
A&A&A&A&A&A&A&A&A&A&A&A&A&A&A&A
\end{array}\right) \pi^{-1}_{\leftarrow} \\
\left(\begin{array}{cccc|cccc|cccc|cccc}
A&A&A&A&P&P&P&P&P&P&P&P&P&P&P&P\\
P&P&P&P&A&A&A&A&P&P&P&P&P&P&P&P\\
P&P&P&P&P&P&P&P&A&A&A&A&P&P&P&P\\
P&P&P&P&P&P&P&P&P&P&P&P&A&A&A&A
\end{array}\right) \kappa_{i-2}\circ\gamma^{-1}\circ\theta_2^{-1} \\
\xleftarrow{} \\
\left(\begin{array}{cccc|cccc|cccc|cccc}
A&A&A&A&P&P&P&P&P&P&P&P&P&P&P&P\\
A&A&A&A&P&P&P&P&P&P&P&P&P&P&P&P\\
A&A&A&A&P&P&P&P&P&P&P&P&P&P&P&P\\
A&A&A&A&P&P&P&P&P&P&P&P&P&P&P&P
\end{array}\right) \pi^{-1}_{\leftarrow} \\
\left(\begin{array}{cccc|cccc|cccc|cccc}
A&P&P&P&P&P&P&P&P&P&P&P&P&P&P&P\\
P&A&P&P&P&P&P&P&P&P&P&P&P&P&P&P\\
P&P&A&P&P&P&P&P&P&P&P&P&P&P&P&P\\
P&P&P&A&P&P&P&P&P&P&P&P&P&P&P&P
\end{array}\right) \kappa_{i-1}\circ\gamma^{-1}\circ\theta_1^{-1} \\
\xleftarrow{} \\
\left(\begin{array}{cccc|cccc|cccc|cccc}
A&P&P&P&P&P&P&P&P&P&P&P&P&P&P&P\\
A&P&P&P&P&P&P&P&P&P&P&P&P&P&P&P\\
A&P&P&P&P&P&P&P&P&P&P&P&P&P&P&P\\
A&P&P&P&P&P&P&P&P&P&P&P&P&P&P&P
\end{array}\right) \pi^{-1}_{\leftarrow} \\
\left(\begin{array}{cccc|cccc|cccc|cccc}
\mathbf{A}&P&P&P&P&P&P&P&P&P&P&P&P&P&P&P\\
P&P&P&P&P&P&P&P&P&P&P&P&P&P&P&P\\
P&P&P&P&P&P&P&P&P&P&P&P&P&P&P&P\\
P&P&P&P&P&P&P&P&P&P&P&P&P&P&P&P
\end{array}\right) \pi\circ\theta_2\circ\gamma\circ\kappa_i \xrightarrow{} \left(\begin{array}{cccc|cccc|cccc|cccc}
A&P&P&P&P&P&P&P&P&P&P&P&P&P&P&P\\
A&P&P&P&P&P&P&P&P&P&P&P&P&P&P&P\\
A&P&P&P&P&P&P&P&P&P&P&P&P&P&P&P\\
A&P&P&P&P&P&P&P&P&P&P&P&P&P&P&P
\end{array}\right) \\
\theta_1\circ\gamma\circ\kappa_{i+1} \xrightarrow{} \left(\begin{array}{cccc|cccc|cccc|cccc}
A&P&P&P&P&P&P&P&P&P&P&P&P&P&P&P\\
P&P&P&A&P&P&P&P&P&P&P&P&P&P&P&P\\
P&P&A&P&P&P&P&P&P&P&P&P&P&P&P&P\\
P&A&P&P&P&P&P&P&P&P&P&P&P&P&P&P
\end{array}\right) \xrightarrow{\pi} \\
\left(\begin{array}{cccc|cccc|cccc|cccc}
A&A&A&A&P&P&P&P&P&P&P&P&P&P&P&P\\
A&A&A&A&P&P&P&P&P&P&P&P&P&P&P&P\\
A&A&A&A&P&P&P&P&P&P&P&P&P&P&P&P\\
A&A&A&A&P&P&P&P&P&P&P&P&P&P&P&P
\end{array}\right) \theta_2\circ\gamma\circ\kappa_{i+2} \xrightarrow{} \left(\begin{array}{cccc|cccc|cccc|cccc}
A&A&A&A&P&P&P&P&P&P&P&P&P&P&P&P\\
P&P&P&P&P&P&P&P&P&P&P&P&A&A&A&A\\
P&P&P&P&P&P&P&P&A&A&A&A&P&P&P&P\\
P&P&P&P&A&A&A&A&P&P&P&P&P&P&P&P
\end{array}\right) \\
\xrightarrow{\pi} \left(\begin{array}{cccc|cccc|cccc|cccc}
A&A&A&A&A&A&A&A&A&A&A&A&A&A&A&A\\
A&A&A&A&A&A&A&A&A&A&A&A&A&A&A&A\\
A&A&A&A&A&A&A&A&A&A&A&A&A&A&A&A\\
A&A&A&A&A&A&A&A&A&A&A&A&A&A&A&A
\end{array}\right) \kappa_{i+4}\circ\pi\circ\theta_1\circ\gamma\circ\kappa_{i+3} \xrightarrow{} \\
\left(\begin{array}{cccc|cccc|cccc|cccc}
B&B&B&B&B&B&B&B&B&B&B&B&B&B&B&B\\
B&B&B&B&B&B&B&B&B&B&B&B&B&B&B&B\\
B&B&B&B&B&B&B&B&B&B&B&B&B&B&B&B\\
B&B&B&B&B&B&B&B&B&B&B&B&B&B&B&B
\end{array}\right)
\end{array}
\tag{6}
$$

Using higher-order multisets, denoted by four A^*, or more precisely, four bytes as a single active 32-bit word, as done in [14] for the AES, we obtain the multiset distinguishers (7) and (8) in the encryption and decryption directions, respectively.

$$\begin{pmatrix} B & B & B & B \\ B & B & B & B \\ B & B & B & B \\ B & B & B & B \end{pmatrix} \begin{pmatrix} B & B & B & B \\ B & B & B & B \\ B & B & B & B \\ B & B & B & B \end{pmatrix} \begin{pmatrix} B & B & B & B \\ B & B & B & B \\ B & B & B & B \\ B & B & B & B \end{pmatrix} \begin{pmatrix} B & B & B & B \\ B & B & B & B \\ B & B & B & B \\ B & B & B & B \end{pmatrix} \theta_2^{-1} \circ \pi^{-1} \circ \kappa_{i-4} \circ \gamma^{-1} \circ \theta_1^{-1}$$

$$\begin{pmatrix} A^* & A^* & A^* & A^* \\ A^* & A^* & A^* & A^* \\ A^* & A^* & A^* & A^* \\ A^* & A^* & A^* & A^* \end{pmatrix} \begin{pmatrix} A^* & A^* & A^* & A^* \\ A^* & A^* & A^* & A^* \\ A^* & A^* & A^* & A^* \\ A^* & A^* & A^* & A^* \end{pmatrix} \begin{pmatrix} A^* & A^* & A^* & A^* \\ A^* & A^* & A^* & A^* \\ A^* & A^* & A^* & A^* \\ A^* & A^* & A^* & A^* \end{pmatrix} \begin{pmatrix} A^* & A^* & A^* & A^* \\ A^* & A^* & A^* & A^* \\ A^* & A^* & A^* & A^* \\ A^* & A^* & A^* & A^* \end{pmatrix} \pi_{\leftarrow}^{-1}$$

$$\begin{pmatrix} A_1^* & A_1^* & A_1^* & A_1^* \\ A_4^* & A_4^* & A_4^* & A_4^* \\ A_3^* & A_3^* & A_3^* & A_3^* \\ A_2^* & A_2^* & A_2^* & A_2^* \end{pmatrix} \begin{pmatrix} A_2^* & A_2^* & A_2^* & A_2^* \\ A_1^* & A_1^* & A_1^* & A_1^* \\ A_4^* & A_4^* & A_4^* & A_4^* \\ A_3^* & A_3^* & A_3^* & A_3^* \end{pmatrix} \begin{pmatrix} A_3^* & A_3^* & A_3^* & A_3^* \\ A_2^* & A_2^* & A_2^* & A_2^* \\ A_1^* & A_1^* & A_1^* & A_1^* \\ A_4^* & A_4^* & A_4^* & A_4^* \end{pmatrix} \begin{pmatrix} A_4^* & A_4^* & A_4^* & A_4^* \\ A_3^* & A_3^* & A_3^* & A_3^* \\ A_2^* & A_2^* & A_2^* & A_2^* \\ A_1^* & A_1^* & A_1^* & A_1^* \end{pmatrix} \kappa_{i-3} \circ \gamma^{-1} \circ \theta_2^{-1}$$

$$\begin{pmatrix} A_1^* & A_1^* & A_1^* & A_1^* \\ A_4^* & A_4^* & A_4^* & A_4^* \\ A_3^* & A_3^* & A_3^* & A_3^* \\ A_2^* & A_2^* & A_2^* & A_2^* \end{pmatrix} \begin{pmatrix} A_2^* & A_2^* & A_2^* & A_2^* \\ A_1^* & A_1^* & A_1^* & A_1^* \\ A_4^* & A_4^* & A_4^* & A_4^* \\ A_3^* & A_3^* & A_3^* & A_3^* \end{pmatrix} \begin{pmatrix} A_3^* & A_3^* & A_3^* & A_3^* \\ A_2^* & A_2^* & A_2^* & A_2^* \\ A_1^* & A_1^* & A_1^* & A_1^* \\ A_4^* & A_4^* & A_4^* & A_4^* \end{pmatrix} \begin{pmatrix} A_4^* & A_4^* & A_4^* & A_4^* \\ A_3^* & A_3^* & A_3^* & A_3^* \\ A_2^* & A_2^* & A_2^* & A_2^* \\ A_1^* & A_1^* & A_1^* & A_1^* \end{pmatrix} \pi_{\leftarrow}^{-1}$$

$$\begin{pmatrix} A^* & P & P & P \\ P & A^* & P & P \\ P & P & A^* & P \\ P & P & P & A^* \end{pmatrix} \begin{pmatrix} A^* & P & P & P \\ P & A^* & P & P \\ P & P & A^* & P \\ P & P & P & A^* \end{pmatrix} \begin{pmatrix} A^* & P & P & P \\ P & A^* & P & P \\ P & P & A^* & P \\ P & P & P & A^* \end{pmatrix} \begin{pmatrix} A^* & P & P & P \\ P & A^* & P & P \\ P & P & A^* & P \\ P & P & P & A^* \end{pmatrix} \kappa_{i-2} \circ \gamma^{-1} \circ \theta_1^{-1}$$

$$\begin{pmatrix} A^* & P & P & P \\ A^* & P & P & P \\ A^* & P & P & P \\ A^* & P & P & P \end{pmatrix} \begin{pmatrix} A^* & P & P & P \\ A^* & P & P & P \\ A^* & P & P & P \\ A^* & P & P & P \end{pmatrix} \begin{pmatrix} A^* & P & P & P \\ A^* & P & P & P \\ A^* & P & P & P \\ A^* & P & P & P \end{pmatrix} \begin{pmatrix} A^* & P & P & P \\ A^* & P & P & P \\ A^* & P & P & P \\ A^* & P & P & P \end{pmatrix} \pi_{\leftarrow}^{-1}$$

$$\begin{pmatrix} A^* & P & P & P \\ P & P & P & P \\ P & P & P & P \\ P & P & P & P \end{pmatrix} \begin{pmatrix} P & P & P & P \\ A^* & P & P & P \\ P & P & P & P \\ P & P & P & P \end{pmatrix} \begin{pmatrix} P & P & P & P \\ P & P & P & P \\ A^* & P & P & P \\ P & P & P & P \end{pmatrix} \begin{pmatrix} P & P & P & P \\ P & P & P & P \\ P & P & P & P \\ A^* & P & P & P \end{pmatrix} \kappa_{i-1} \circ \gamma^{-1} \circ \theta_2^{-1} \circ \pi^{-1}$$

$$\begin{pmatrix} A^* & P & P & P \\ A^* & P & P & P \\ A^* & P & P & P \\ A^* & P & P & P \end{pmatrix} \begin{pmatrix} P & P & P & P \\ P & P & P & P \\ P & P & P & P \\ P & P & P & P \end{pmatrix} \begin{pmatrix} P & P & P & P \\ P & P & P & P \\ P & P & P & P \\ P & P & P & P \end{pmatrix} \begin{pmatrix} P & P & P & P \\ P & P & P & P \\ P & P & P & P \\ P & P & P & P \end{pmatrix} \tag{7}$$

$$\begin{pmatrix} A^* & P & P & P \\ P & A^* & P & P \\ P & P & A^* & P \\ P & P & P & A^* \end{pmatrix} \begin{pmatrix} P & P & P & P \\ P & P & P & P \\ P & P & P & P \\ P & P & P & P \end{pmatrix} \begin{pmatrix} P & P & P & P \\ P & P & P & P \\ P & P & P & P \\ P & P & P & P \end{pmatrix} \begin{pmatrix} P & P & P & P \\ P & P & P & P \\ P & P & P & P \\ P & P & P & P \end{pmatrix} \pi \circ \theta_1 \circ \gamma \circ \kappa_i$$

$$\begin{pmatrix} A^* & P & P & P \\ A^* & P & P & P \\ A^* & P & P & P \\ A^* & P & P & P \end{pmatrix} \begin{pmatrix} P & P & P & P \\ P & P & P & P \\ P & P & P & P \\ P & P & P & P \end{pmatrix} \begin{pmatrix} P & P & P & P \\ P & P & P & P \\ P & P & P & P \\ P & P & P & P \end{pmatrix} \begin{pmatrix} P & P & P & P \\ P & P & P & P \\ P & P & P & P \\ P & P & P & P \end{pmatrix} \theta_2 \circ \gamma \circ \kappa_{i+1}$$

$$\begin{pmatrix} A^* & P & P & P \\ P & P & P & P \\ P & P & P & P \\ P & P & P & P \end{pmatrix} \begin{pmatrix} P & P & P & P \\ P & P & P & P \\ P & P & P & P \\ A^* & P & P & P \end{pmatrix} \begin{pmatrix} P & P & P & P \\ P & P & P & P \\ P & P & P & P \\ P & P & P & P \end{pmatrix} \begin{pmatrix} P & P & P & P \\ A^* & P & P & P \\ P & P & P & P \\ P & P & P & P \end{pmatrix} \pi$$

$$\begin{pmatrix} A^* & P & P & P \\ A^* & P & P & P \\ A^* & P & P & P \\ A^* & P & P & P \end{pmatrix} \begin{pmatrix} A^* & P & P & P \\ A^* & P & P & P \\ A^* & P & P & P \\ A^* & P & P & P \end{pmatrix} \begin{pmatrix} A^* & P & P & P \\ A^* & P & P & P \\ A^* & P & P & P \\ A^* & P & P & P \end{pmatrix} \begin{pmatrix} A^* & P & P & P \\ A^* & P & P & P \\ A^* & P & P & P \\ A^* & P & P & P \end{pmatrix} \theta_1 \circ \gamma \circ \kappa_{i+2}$$

$$\begin{pmatrix} A^* & P & P & P \\ P & P & P & A^* \\ P & P & A^* & P \\ P & A^* & P & P \end{pmatrix} \begin{pmatrix} A^* & P & P & P \\ P & P & P & A^* \\ P & P & A^* & P \\ P & A^* & P & P \end{pmatrix} \begin{pmatrix} A^* & P & P & P \\ P & P & P & A^* \\ P & P & A^* & P \\ P & A^* & P & P \end{pmatrix} \begin{pmatrix} P & P & P & P \\ P & P & P & A^* \\ P & P & A^* & P \\ P & A^* & P & P \end{pmatrix} \pi$$

$$\begin{pmatrix} A_1^* & A_1^* & A_1^* & A_1^* \\ A_4^* & A_4^* & A_4^* & A_4^* \\ A_3^* & A_3^* & A_3^* & A_3^* \\ A_2^* & A_2^* & A_2^* & A_2^* \end{pmatrix} \begin{pmatrix} A_2^* & A_2^* & A_2^* & A_2^* \\ A_1^* & A_1^* & A_1^* & A_1^* \\ A_4^* & A_4^* & A_4^* & A_4^* \\ A_3^* & A_3^* & A_3^* & A_3^* \end{pmatrix} \begin{pmatrix} A_3^* & A_3^* & A_3^* & A_3^* \\ A_2^* & A_2^* & A_2^* & A_2^* \\ A_1^* & A_1^* & A_1^* & A_1^* \\ A_4^* & A_4^* & A_4^* & A_4^* \end{pmatrix} \begin{pmatrix} A_4^* & A_4^* & A_4^* & A_4^* \\ A_3^* & A_3^* & A_3^* & A_3^* \\ A_2^* & A_2^* & A_2^* & A_2^* \\ A_1^* & A_1^* & A_1^* & A_1^* \end{pmatrix} \theta_2 \circ \gamma \circ \kappa_{i+3}$$

$$\begin{pmatrix} A_2^* & A_2^* & A_2^* & A_2^* \\ A_1^* & A_1^* & A_1^* & A_1^* \\ A_4^* & A_4^* & A_4^* & A_4^* \\ A_3^* & A_3^* & A_3^* & A_3^* \end{pmatrix} \begin{pmatrix} A_3^* & A_3^* & A_3^* & A_3^* \\ A_2^* & A_2^* & A_2^* & A_2^* \\ A_1^* & A_1^* & A_1^* & A_1^* \\ A_4^* & A_4^* & A_4^* & A_4^* \end{pmatrix} \begin{pmatrix} A_4^* & A_4^* & A_4^* & A_4^* \\ A_3^* & A_3^* & A_3^* & A_3^* \\ A_2^* & A_2^* & A_2^* & A_2^* \\ A_1^* & A_1^* & A_1^* & A_1^* \end{pmatrix} \begin{pmatrix} A_1^* & A_1^* & A_1^* & A_1^* \\ A_4^* & A_4^* & A_4^* & A_4^* \\ A_3^* & A_3^* & A_3^* & A_3^* \\ A_2^* & A_2^* & A_2^* & A_2^* \end{pmatrix} \theta_1 \circ \gamma \circ \kappa_{i+4} \circ \pi$$

$$\begin{pmatrix} A^* & A^* & A^* & A^* \\ A^* & A^* & A^* & A^* \\ A^* & A^* & A^* & A^* \\ A^* & A^* & A^* & A^* \end{pmatrix} \begin{pmatrix} A^* & A^* & A^* & A^* \\ A^* & A^* & A^* & A^* \\ A^* & A^* & A^* & A^* \\ A^* & A^* & A^* & A^* \end{pmatrix} \begin{pmatrix} A^* & A^* & A^* & A^* \\ A^* & A^* & A^* & A^* \\ A^* & A^* & A^* & A^* \\ A^* & A^* & A^* & A^* \end{pmatrix} \begin{pmatrix} A^* & A^* & A^* & A^* \\ A^* & A^* & A^* & A^* \\ A^* & A^* & A^* & A^* \\ A^* & A^* & A^* & A^* \end{pmatrix} \kappa_{i+5} \circ \pi$$

$$\begin{pmatrix} B & B & B & B \\ B & B & B & B \\ B & B & B & B \\ B & B & B & B \end{pmatrix} \begin{pmatrix} B & B & B & B \\ B & B & B & B \\ B & B & B & B \\ B & B & B & B \end{pmatrix} \begin{pmatrix} B & B & B & B \\ B & B & B & B \\ B & B & B & B \\ B & B & B & B \end{pmatrix} \begin{pmatrix} B & B & B & B \\ B & B & B & B \\ B & B & B & B \\ B & B & B & B \end{pmatrix} \tag{8}$$

Analogous to [14], the 5.25-round forward and 4.5-round backward multisets (7) and (8) can be combined over 9.75-round 3D. We construct a structure of $2^{(4+3)*8} = 2^{56}$ CP which differ in the seven bytes depicted in (9), and constant bytes in the remaining positions of the state. This can be viewed as a collection of 2^{24} copies of the forward multiset, or a collection of 2^{24} copies of the backward multiset. Combining both multisets, exactly as in [14], one records the frequencies in each byte of plaintext and ciphertext and checks if the values in each byte of plaintext and ciphertext of a 2^{32} multiset is balanced (zeroxor sum). The time complexity is 2^{56} 9.75-round encryptions, 2^{56} CP and small memory (just to keep track if the xor sum is zero).

$$\left(\begin{array}{cccc|cccc|cccc|cccc} B & B & B & B & B & B & B & B & B & B & B & B & B & B & B & B \\ B & B & B & B & B & B & B & B & B & B & B & B & B & B & B & B \\ B & B & B & B & B & B & B & B & B & B & B & B & B & B & B & B \\ B & B & B & B & B & B & B & B & B & B & B & B & B & B & B & B \end{array}\right) \xleftarrow{4.5 \text{ rounds}}$$

$$\left(\begin{array}{cccc|cccc|cccc|cccc} A^* & P & P & P & P & P & P & P & P & P & P & P & P & P & P & P \\ A^* & A^* & P & P & P & P & P & P & P & P & P & P & P & P & P & P \\ A^* & P & A^* & P & P & P & P & P & P & P & P & P & P & P & P & P \\ A^* & P & P & A^* & P & P & P & P & P & P & P & P & P & P & P & P \end{array}\right) \xrightarrow{5.25 \text{ rounds}}$$

$$\left(\begin{array}{cccc|cccc|cccc|cccc} B & B & B & B & B & B & B & B & B & B & B & B & B & B & B & B \\ B & B & B & B & B & B & B & B & B & B & B & B & B & B & B & B \\ B & B & B & B & B & B & B & B & B & B & B & B & B & B & B & B \\ B & B & B & B & B & B & B & B & B & B & B & B & B & B & B & B \end{array}\right) \tag{9}$$

6 Conclusions

This paper presented new known-key and ID distinguishers for the 3D block cipher [17], along with distinguishing and key-recovery attacks. These distinguishers cover more rounds than any previously reported one, and allow to perform better attacks on reduced-round versions of the 3D cipher, either starting from an odd-numbered or an even-numbered round, depending on the use of θ_1 or θ_2 transformations.

The ID attacks were possible due to new ideas in [1] using ID distinguishers $\alpha \overset{6r}{\nrightarrow} \eta$ with low Hamming weight of byte differences, for both α and η. Traditional ID attacks, such as [4] could not profit from these new ID distinguishers because there would be not enough pairs surviving the filtering due to the large number of zero byte differences in η.

Known-key distinguishers covering 7.75 and 9.75 rounds of 3D were described in Sect. 5. The impact of known-key attacks on reduced-round 3D is, for instance, to show that r-round 3D does not behave as an ideal cryptographic primitive, such as a random function or random permutation in settings where the key input is under the control of the adversary, such as in hash functions.

Table 1 lists the complexities of previous and new attacks described in this paper. A distinguishing-from-random ID attack on 6-round 3D is described in the appendix. The attacks detailed in this paper are the currently best ones on reduced-round versions the 3D block cipher in the single-key model, even though the attack complexities are not practical. Also, although our attacks reach almost double the numbers of rounds of previous analyses [17], they do not threaten the full 22-round 3D cipher. The security margin is still high. A

Table 1. Attack complexities on reduced-round 3D cipher

Attack	Time	Data	Memory	#Rounds	Source
Multiset	$2^{19.5}$	2^9 CP	2^8	4.75	[17]
ID	$2^{65.5}$	2^{36} CP	2^{32}	5.75	[17]
Multiset	2^{139}	2^{129} CP	2^{128}	5.75	[17]
ID	2^{256}	2^{256} CC	2^{256}	6	appendix A
Known-key	2^8	2^8 CP	negligible	7.75	see (5)
Known-key	2^{56}	2^{56} CP	negligible	9.75	see (9)
ID	2^{401}	2^{501} CP	2^{311}	10	see (4)

Time complexity in number of encryptions; memory complexity in number of text blocks
CP: Chosen Plaintext; CC: Chosen Ciphertext

promising future research direction is to apply related-key attacks on 3D or reduced-round versions, due to the similarity between 3D and the AES.

References

1. Barak, B., Aref, M.R.: Impossible Differential Attack on seven-round AES-128. IET Information Security 2(2), 28–32 (2008)
2. Barkan, E., Biham, E.: In how many ways can you write Rijndael?, IACR ePrint archive 2002/157 (2002)
3. Biham, E., Biryukov, A., Shamir, A.: Cryptanalysis of Skipjack Reduced to 31 Rounds using Impossible Differentials. In: Stern, J. (ed.) EUROCRYPT 1999. LNCS, vol. 1592, pp. 12–23. Springer, Heidelberg (1999)
4. Biham, E., Biryukov, A., Shamir, A.: Miss in the Middle Attacks on IDEA and Khufu. In: Knudsen, L.R. (ed.) FSE 1999. LNCS, vol. 1636, pp. 124–138. Springer, Heidelberg (1999)
5. Biham, E., Furman, V.: Improved Impossible Differentials on Twofish. In: Roy, B., Okamoto, E. (eds.) INDOCRYPT 2000. LNCS, vol. 1977, pp. 80–92. Springer, Heidelberg (2000)
6. Biham, E., Keller, N.: Cryptanalysis of Reduced Variants of Rijndael. In: Proceedings of the 3rd AES Conference (2000)
7. Cheon, J.H., Kim, M., Kim, K.: Impossible Differential Cryptanalysis of Hierocrypt-3 Reduced to 3 Rounds. In: Proceedings of 2nd NESSIE Workshop (2001)
8. Cheon, J.H., Kim, M., Kim, K., Lee, J.Y., Kang, S.: Improved Impossible Differential Cryptanalysis of Rijndael and Crypton. In: Kim, K.-c. (ed.) ICISC 2001. LNCS, vol. 2288, pp. 39–49. Springer, Heidelberg (2002)
9. Daemen, J., Rijmen, V.: The Design of Rijndael: AES - The Advanced Encryption Standard. Springer, Heidelberg (2002)
10. Daemen, J., Knudsen, L.R., Rijmen, V.: The Block Cipher Square. In: Biham, E. (ed.) FSE 1997. LNCS, vol. 1267, pp. 149–165. Springer, Heidelberg (1997)
11. FIPS197: Advanced Encryption Standard (AES). FIPS PUB 197 Federal Information Processing Standard Publication 197, U.S. Department of Commerce (2001)
12. Hong, D., Sung, J., Moriai, S., Lee, S., Lim, J.: Impossible differential cryptanalysis of zodiac. In: Matsui, M. (ed.) FSE 2001. LNCS, vol. 2355, pp. 300–311. Springer, Heidelberg (2002)

13. Knudsen, L.R.: DEAL – a 128-bit Block Cipher. Technical Report #151, University of Bergen, Dept. of Informatics, Norway (1998)
14. Knudsen, L.R., Rijmen, V.: Known-key Distinguishers for some Block Ciphers. In: Kurosawa, K. (ed.) ASIACRYPT 2007. LNCS, vol. 4833, pp. 315–324. Springer, Heidelberg (2007)
15. Menezes, A.J., van Oorschot, P.C., Vanstone, S.A.: Handbook of Applied Cryptography. CRC Press, Boca Raton (1997)
16. Moon, D., Hwang, K., Lee, W., Lee, S., Lim, J.: Impossible Differential Cryptanalysis of Reduced Round XTEA and TEA. In: Daemen, J., Rijmen, V. (eds.) FSE 2002. LNCS, vol. 2365, pp. 49–60. Springer, Heidelberg (2002)
17. Nakahara Jr., J.: 3D: a Three-Dimensional Block Cipher. In: Franklin, M.K., Hui, L.C.K., Wong, D.S. (eds.) CANS 2008. LNCS, vol. 5339, pp. 252–267. Springer, Heidelberg (2008)

A A Distinguishing Attack

We slightly change (2) so that the difference pattern in η contains thirty-two Δ bytes, and call this 6-round ID distinguisher (10). This CC attack is motivated by the fact that $\alpha \not\rightarrow \eta$ if and only if $\eta \not\rightarrow \alpha$.

$$
\alpha = \left(\begin{array}{c|c|c|c} \Delta\,0\,0\,0 & 0\,0\,0\,0 & 0\,0\,0\,0 & 0\,0\,0\,0 \\ 0\,0\,0\,0 & 0\,0\,0\,0 & 0\,0\,0\,0 & 0\,0\,0\,0 \\ 0\,0\,0\,0 & 0\,0\,0\,0 & 0\,0\,0\,0 & 0\,0\,0\,0 \\ 0\,0\,0\,0 & 0\,0\,0\,0 & 0\,0\,0\,0 & 0\,0\,0\,0 \end{array}\right)
\overset{\pi\circ\theta_1\circ\gamma\circ\kappa_i}{\rightarrow}
\left(\begin{array}{c|c|c|c} \Delta\,0\,0\,0 & 0\,0\,0\,0 & 0\,0\,0\,0 & 0\,0\,0\,0 \\ \Delta\,0\,0\,0 & 0\,0\,0\,0 & 0\,0\,0\,0 & 0\,0\,0\,0 \\ \Delta\,0\,0\,0 & 0\,0\,0\,0 & 0\,0\,0\,0 & 0\,0\,0\,0 \\ \Delta\,0\,0\,0 & 0\,0\,0\,0 & 0\,0\,0\,0 & 0\,0\,0\,0 \end{array}\right)
$$

$$
\overset{\theta_2\circ\gamma\circ\kappa_{i+1}}{\rightarrow}
\left(\begin{array}{c|c|c|c} \Delta\,0\,0\,0 & 0\,0\,0\,0 & 0\,0\,0\,0 & 0\,0\,0\,0 \\ 0\,0\,0\,0 & 0\,0\,0\,0 & 0\,0\,0\,0 & \Delta\,0\,0\,0 \\ 0\,0\,0\,0 & 0\,0\,0\,0 & \Delta\,0\,0\,0 & 0\,0\,0\,0 \\ 0\,0\,0\,0 & \Delta\,0\,0\,0 & 0\,0\,0\,0 & 0\,0\,0\,0 \end{array}\right)
\overset{\pi}{\rightarrow}
\left(\begin{array}{c|c|c|c} \Delta\,0\,0\,0 & \Delta\,0\,0\,0 & \Delta\,0\,0\,0 & \Delta\,0\,0\,0 \\ \Delta\,0\,0\,0 & \Delta\,0\,0\,0 & \Delta\,0\,0\,0 & \Delta\,0\,0\,0 \\ \Delta\,0\,0\,0 & \Delta\,0\,0\,0 & \Delta\,0\,0\,0 & \Delta\,0\,0\,0 \\ \Delta\,0\,0\,0 & \Delta\,0\,0\,0 & \Delta\,0\,0\,0 & \Delta\,0\,0\,0 \end{array}\right)
$$

$$
\overset{\theta_1\circ\gamma\circ\kappa_{i+2}}{\rightarrow}
\left(\begin{array}{c|c|c|c} \Delta\,0\,0\,0 & \Delta\,0\,0\,0 & \Delta\,0\,0\,0 & \Delta\,0\,0\,0 \\ 0\,0\,0\,\Delta & 0\,0\,0\,\Delta & 0\,0\,0\,\Delta & 0\,0\,0\,\Delta \\ 0\,0\,\Delta\,0 & 0\,0\,\Delta\,0 & 0\,0\,\Delta\,0 & 0\,0\,\Delta\,0 \\ 0\,\Delta\,0\,0 & 0\,\Delta\,0\,0 & 0\,\Delta\,0\,0 & 0\,\Delta\,0\,0 \end{array}\right)
\overset{\pi}{\rightarrow}
$$

$$
\left(\begin{array}{c|c|c|c} \Delta\,\Delta\,\Delta\,\Delta & \Delta\,\Delta\,\Delta\,\Delta & \Delta\,\Delta\,\Delta\,\Delta & \Delta\,\Delta\,\Delta\,\Delta \\ \Delta\,\Delta\,\Delta\,\Delta & \Delta\,\Delta\,\Delta\,\Delta & \Delta\,\Delta\,\Delta\,\Delta & \Delta\,\Delta\,\Delta\,\Delta \\ \Delta\,\Delta\,\Delta\,\Delta & \Delta\,\Delta\,\Delta\,\Delta & \Delta\,\Delta\,\Delta\,\Delta & \Delta\,\Delta\,\Delta\,\Delta \\ \Delta\,\Delta\,\Delta\,\Delta & \Delta\,\Delta\,\Delta\,\Delta & \Delta\,\Delta\,\Delta\,\Delta & \Delta\,\Delta\,\Delta\,\Delta \end{array}\right)
\overset{\theta_2\circ\gamma\circ\kappa_{i+3}}{\rightarrow}
$$

$$
\left(\begin{array}{c|c|c|c} \Delta\,\Delta\,\Delta\,\Delta & \Delta\,\Delta\,\Delta\,\Delta & \Delta\,\Delta\,\Delta\,\Delta & \Delta\,\Delta\,\Delta\,\Delta \\ \Delta\,\Delta\,\Delta\,\Delta & \Delta\,\Delta\,\Delta\,\Delta & \Delta\,\Delta\,\Delta\,\Delta & \Delta\,\Delta\,\Delta\,\Delta \\ \Delta\,\Delta\,\Delta\,\Delta & \Delta\,\Delta\,\Delta\,\Delta & \Delta\,\Delta\,\Delta\,\Delta & \Delta\,\Delta\,\Delta\,\Delta \\ \Delta\,\Delta\,\Delta\,\Delta & \Delta\,\Delta\,\Delta\,\Delta & \Delta\,\Delta\,\Delta\,\Delta & \Delta\,\Delta\,\Delta\,\Delta \end{array}\right)
\overset{\pi}{\not\rightarrow}
$$

$$
\left(\begin{array}{c|c|c|c} 0\,0\,0\,0 & 0\,0\,0\,0 & ?\,?\,?\,? & ?\,?\,?\,? \\ 0\,0\,0\,0 & 0\,0\,0\,0 & ?\,?\,?\,? & ?\,?\,?\,? \\ 0\,0\,0\,0 & 0\,0\,0\,0 & ?\,?\,?\,? & ?\,?\,?\,? \\ 0\,0\,0\,0 & 0\,0\,0\,0 & ?\,?\,?\,? & ?\,?\,?\,? \end{array}\right)
\overset{\kappa_{i+4}\circ\gamma^{-1}\circ\theta_1^{-1}\circ\pi^{-1}}{\leftarrow}
$$

$$
\left(\begin{array}{c|c|c|c} 0\,0\,0\,0 & 0\,0\,0\,0 & \Delta\,\Delta\,\Delta\,\Delta & \Delta\,\Delta\,\Delta\,\Delta \\ 0\,0\,0\,0 & 0\,0\,0\,0 & \Delta\,\Delta\,\Delta\,\Delta & \Delta\,\Delta\,\Delta\,\Delta \\ 0\,0\,0\,0 & 0\,0\,0\,0 & \Delta\,\Delta\,\Delta\,\Delta & \Delta\,\Delta\,\Delta\,\Delta \\ 0\,0\,0\,0 & 0\,0\,0\,0 & \Delta\,\Delta\,\Delta\,\Delta & \Delta\,\Delta\,\Delta\,\Delta \end{array}\right)
$$

$$
\overset{\kappa_{i+5}\circ\gamma^{-1}\circ\theta_2^{-1}\circ\kappa_{i+6}}{\leftarrow}
\left(\begin{array}{c|c|c|c} 0\,0\,0\,0 & 0\,0\,0\,0 & \Delta\,\Delta\,\Delta\,\Delta & \Delta\,\Delta\,\Delta\,\Delta \\ 0\,0\,0\,0 & \Delta\,\Delta\,\Delta\,\Delta & \Delta\,\Delta\,\Delta\,\Delta & 0\,0\,0\,0 \\ \Delta\,\Delta\,\Delta\,\Delta & \Delta\,\Delta\,\Delta\,\Delta & 0\,0\,0\,0 & 0\,0\,0\,0 \\ \Delta\,\Delta\,\Delta\,\Delta & 0\,0\,0\,0 & 0\,0\,0\,0 & \Delta\,\Delta\,\Delta\,\Delta \end{array}\right) = \eta
\tag{10}
$$

The distinguisher (10) can be used in a chosen-ciphertext (CC) setting, for instance, to distinguish 6-round 3D (or a dual cipher [2]) from a random permutation. The procedure is the following:

(i) choose $(2^8)^{32} = 2^{256}$ ciphertexts C_i, whose bytes in the thirty-two Δ bytes differences in the ciphertext pattern assume all possible 256-bit values, while the remaining bytes are (arbitrary) constants;
(ii) request the decryption of the C_i's across six rounds, and store the corresponding plaintexts P_i, $0 \leq i \leq 2^{256} - 1$;
(iii) form $2^{256}(2^{256} - 1)/2 \approx 2^{511}$ pairs $P_i \oplus P_j$, $i \neq j$;
(iv) if no pair $P_i \oplus P_j$ has a single nonzero byte difference, then the cipher is identified as 6-round 3D (or a dual cipher); otherwise, it is considered a random permutation. There are 64 possible positions for the single nonzero byte difference in the plaintext state. Thus, the joint probability of these plaintext difference patterns is $64 \cdot (2^{-8})^{63} = 2^{6-504} = 2^{-498}$. There is a chance of 2^{-498} that a single-byte difference in any of the 64 state positions in (10) is satisfied by a random permutation. Thus, $1 - 2^{-498}$ is the probability that it is not satisfied by a single pair. For t pairs, the probability that the difference pattern does not appears in a random permutation is $(1 - 2^{-498})^t \approx e^{-t/2^{498}}$. Using $t = 2^{511}$ pairs there is a chance of $1/e^{8192} \approx 2^{-11818}$ that the output difference of (10) does not appears in a random permutation.

There is no shortage of pairs for this attack. For a random permutation, the 2^{511} pairs lead to about $2^{511} \cdot 2^{-498} = 2^{13}$ pairs potentially satisfying a plaintext difference pattern with a single nonzero byte difference. This distinguishing attack costs 2^{256} 6-round decryptions, 2^{256} chosen ciphertexts (CC) and equivalent memory.